Chapter 1:

# Privacy Safeguard 1 —

## Open and transparent management of CDR data

Consultation draft, October 2019



OAIC

# Contents

# Key points

- Privacy Safeguard 1, together with Consumer Data Rule 7.2, outlines the requirements for all Consumer Data Right (CDR) entities (accredited data recipients, data holders and designated gateways) to handle CDR data in an open and transparent way.
- All CDR entities must take steps as are reasonable in the circumstances to implement practices, procedures and systems that will ensure they comply with the CDR regime, and are able to deal with related inquiries and complaints from consumers.
- All CDR entities must have a clearly expressed and up-to-date policy about how they manage CDR data. The policy must be provided free of charge and made available in accordance with the Consumer Data Rules.

# What does Privacy Safeguard 1 say?

1.1 Privacy Safeguard 1 requires all CDR entities to:

- take steps that are reasonable in the circumstances to establish and maintain internal practices, procedures and systems that ensure compliance with the CDR regime, including the Privacy Safeguards and Consumer Data Rules and
- have a clearly expressed and up-to-date policy describing how they manage CDR data. The policy must be available free of charge and in a form consistent with the Consumer Data Rules and provided to the consumer upon request.

# Importance of open and transparent management of CDR data

1.2 The objective of Privacy Safeguard 1 is to ensure CDR entities handle CDR data in an open and transparent way. It is the bedrock principle.

1.3 By complying with this Privacy Safeguard, CDR entities will be establishing an accountable and auditable practice procedures and systems that will assist in complying with all the other Privacy Safeguards. This leads to a trickle-down effect where privacy is automatically considered when handling CDR data, resulting in better overall privacy management, practice and compliance through a "privacy by design" approach.

1.4 It is also important that consumers are aware of how their CDR data is handled, and can inquire or make complaints to resolve their concerns. A CDR Policy achieves this transparency by outlining how the CDR entity manages CDR data, and by providing information on how a consumer can complain and how the CDR entity will deal with a complaint.

# Who Privacy Safeguard 1 applies to

1.5 Privacy Safeguard 1 applies to data holders, designated gateways and accredited data recipients.

# How Privacy Safeguard 1 interacts with the Privacy Act and APP1

1.6 It is important to understand how Privacy Safeguard 1 interacts with the *Privacy Act 1988* (the Privacy Act) and Australian Privacy Principle (APP) 1.[1]

1.7 Like Privacy Safeguard 1, APP 1 provides certain obligations that require APP entities to manage personal information in an open and transparent way (see Chapter 1: Open and transparent management of personal information of the APP Guidelines).

## Summary of application of Privacy Safeguard 1 by CDR entity

| CDR entity | Privacy principle that applies to CDR data |
|---|---|
| **Accredited person** | **Australian Privacy Principle 1 and Privacy Safeguard 1**<br><br>Privacy Safeguard 1 applies in parallel with APP 1. This means that accredited persons must, at all times, have systems, practices and procedures to comply with both the Privacy Safeguards and the APPs (including having both a CDR policy and Privacy Policy in place,) regardless of whether CDR data has been transferred. |
| **Accredited data recipient** | **Privacy Safeguard 1**<br><br>Privacy Safeguard 1 applies instead of APP 1, meaning APP 1 will not apply to CDR data an accredited data recipient receives through the CDR regime.<br><br>APP 1 will continue to apply to any personal information handled by the accredited data recipient that is not CDR data.[2] This is because all accredited data recipients are subject to the Privacy Act and the APPs for any personal information, even if it is not CDR data. |
| **Designated gateway** | **Australian Privacy Principle 1 and Privacy Safeguard 1**<br><br>Privacy Safeguard 1 applies in parallel with APP 1. This means that a designated gateway must, at all times, have systems, practices and procedures to comply with both the Privacy Safeguards and the APPs (including having both a CDR policy and a Privacy Policy in place), regardless of whether CDR data has been transferred. |
| **Data holder** | **Australian Privacy Principle 1 and Privacy Safeguard 1**<br><br>Privacy Safeguard 1 applies in parallel with APP 1. This means that a data holder must, at all times, have systems, practices and procedures to comply with both the Privacy Safeguards and the APPs, and have a CDR policy and a Privacy Policy in place, regardless of whether CDR data has been transferred. |

[1] The Privacy Act includes 13 APPs that regulate the handling of personal information by APP entities. See Chapter B: Key concepts of the APP Guidelines for further information.

[2] See s 6E(1D) of the Privacy Act.

# Implementing practices, procedures and systems to ensure compliance with the CDR regime

1.8 Privacy Safeguard 1 requires all CDR entities to take steps that are reasonable in the circumstances to establish and maintain internal practices, procedures and systems that:

- ensure compliance with the CDR regime, including the Privacy Safeguards and the Consumer Data Rules, and
- enable the entity to deal with inquiries or complaints from consumers about the entity's compliance with the CDR regime, including the Privacy Safeguards and Consumer Data Rules.

1.9 This is a distinct and separate obligation upon a CDR entity, in addition to being a general statement of its obligation to comply with the CDR regime.

1.10 The Consumer Data Rules contain several governance mechanisms, policies and procedures that will assist entities to take steps that are reasonable to comply with the CDR regime.[3] However, while compliance with the Consumer Data Rules will assist entities to take steps that are reasonable, this does not of itself mean that the entity has complied with Privacy Safeguard 1.

1.11 To comply with Privacy Safeguard 1, CDR entities need to proactively consider, plan and address how to implement any practices, procedures and systems under the Privacy Safeguards and the Consumer Data Rules (including how these interact with other obligations). This should occur before the entity first starts participating in the CDR regime.

1.12 Compliance with Privacy Safeguard 1 should therefore be understood as a matter of good governance.

**Risk point**: Entities who implement the requirements of the Privacy Safeguards and the Consumer Data Rules in isolation or at a late stage risk unnecessary costs or inadequate solutions that fail to address the full compliance picture.

**Privacy tip**: Entities should embed 'privacy-by-design' in relation to handling CDR data across and within their organisation. This ensures CDR requirements are considered holistically. The OAIC has a range of tools to assist entities develop their wider privacy program, including the Privacy management framework.

## Existing privacy governance arrangements

1.13 Where an entity has existing privacy practices and procedures for personal information it handles under the Privacy Act, it may be appropriate to extend these to its CDR data.

1.14 However, the mere extension of current practices and procedures does not mean in and of itself that an entity has taken *reasonable steps* to implement practices, procedures and systems.

[3] For example, accredited data recipients are required to establish a formal governance framework for managing information security risks under the Privacy Safeguard 12 Consumer Data Rules.

1.15 Entities will need to take further action to modify practices, procedures and systems to meet obligations under Privacy Safeguard 1 to ensure compliance with the particularities of the CDR regime.

## Examples of practices, procedures and systems

1.16 The following are given as examples of practices, procedures and systems that a CDR entity should consider implementing under Privacy Safeguard 1.

1.17 These examples may overlap and interact with existing requirements set out by the Consumer Data Rules or the draft ACCC CDR Accreditation Guidelines.

### Have a CDR data management plan

1.18 In practice, CDR entities should develop a CDR management plan or CDR management framework which identifies goals and targets, appoints key roles and responsibilities for privacy management, and adopts governance mechanisms to bring their privacy planning together.

1.19 Entities should proactively review and audit the adequacy and currency of their organisational practices, procedures and systems involving CDR data.

1.20 Where entities have an existing Privacy Management Plan, they may wish to update it with CDR activities so that it is integrated into the entity's privacy management processes, or they may have a separate CDR management plan.

1.21 A CDR entity should also regularly review and update this CDR data management plan to ensure that it reflects the entity's CDR data privacy goals and handling practices.

**What is a CDR data management plan?**

A CDR data management plan can be a helpful way to identify specific, measurable goals and targets, and sets out how an entity will meet its compliance obligations under Privacy Safeguard 1. The CDR data management plan should also include processes to measure and document the CDR entity's performance against their CDR data management plan.

### Embed a culture that respects and protects CDR data

1.22 Good CDR data management stems from good privacy governance. Entities should ensure leadership and governance arrangements create a culture of privacy that respects and protects CDR data.

1.23 To embed a culture of privacy, entities could:

- Appoint a member of senior management to be responsible for the strategic leadership and overall privacy management of CDR data.
- Appoint an officer (or officers) to be responsible for the day to day managing, advising and reporting on Privacy Safeguard issues.
- Record and report on how datasets containing CDR data are treated, managed and protected.
- Implement reporting mechanisms that ensure senior management are routinely informed about privacy issues.

## Establish robust and effective privacy practices, procedures and systems

1.24 Good privacy management requires the development and implementation of robust and effective practices, procedures and systems.

1.25 For example, an entity could:

- Implement risk management processes that allow identification, assessment and management of privacy risks, including CDR security risks.[4]
- Establish clear processes for reviewing and responding to CDR data complaints.
- Integrate Privacy Safeguards training into induction processes and provide regular staff training to those who deal with CDR data. This regular training should occur at a minimum once per year.[5]
- Establish processes that allow consumers to promptly and easily access and correct their CDR data, in accordance with the Consumer Data Rules.

## Regularly reviewing and evaluating privacy processes

1.26 To evaluate privacy practices, procedures and systems, entities should make a commitment to:

- Monitor and review CDR privacy processes regularly. This could include assessing the adequacy and currency of practices, procedures and systems, to ensure they are up to date and being adhered to.
- Measure performance against the CDR data management plan.
- Create feedback channels for both staff and consumers to continue to learn lessons from complaints and breaches, as well as customer feedback more generally.

## Enhance response to privacy issues

1.27 Good privacy management requires entities to be proactive, forward thinking and to anticipate future challenges. To enhance response to privacy issues, entities should make a commitment to:

- Use the results of the evaluations to make necessary and appropriate changes to organisation's practices, procedures and systems.
- Consider having practices, procedures and systems externally assessed to identify areas where privacy processes may be improved.[6]

---

[4] Accredited data recipients are already required to meet strong minimum information security controls under Privacy Safeguard 12. See Schedule 2 of the Consumer Data Rules and the ACCC's *draft Supplementary accreditation guidelines: information security* available on the ACCC's CDR draft accreditation guidelines page.

[5] Accredited data recipients already have certain obligations to provide privacy and security training under Privacy Safeguard 12. See Schedule 2 of the Consumer Data Rules and the ACCC's *draft Supplementary accreditation guidelines: information security* available on the ACCC's CDR draft accreditation guidelines page.

[6] Accredited persons have obligations to provide regulate assurance reports (an audit report) and attestation statements concerning compliance with certain Privacy Safeguard 12 Consumer Data Rules. See the ACCC's *draft Supplementary accreditation guidelines: information security* available on the ACCC's CDR draft accreditation guidelines page.

- Continuously monitor and address new privacy risks.

## Circumstances that affect reasonable steps

1.28 The requirement to implement practices, procedures and systems is qualified by a 'reasonable steps' test.

1.29 This requires an objective assessment of what is considered reasonable in the specific circumstance, which could include:

- the Consumer Data Rules and other legislative obligations that apply to the CDR entity
- the nature of the CDR entity
- the amount of CDR data handled by the CDR entity
- the possible adverse consequences for a consumer in the case of a breach
- the practicability, including time and cost involved.

### The CDR regime obligations that apply to the CDR entity

1.30 The CDR regime obligations (such as the Privacy Safeguards and the Consumer Data Rules) that apply to the entity will be relevant to determining what steps will be reasonable. For example, an accredited data recipient will need to put in place different mechanisms than a data holder to ensure it is compliant with the CDR regime.

### Nature of the entity

1.31 The size of the CDR entity, its resources, the complexity of its operations and the business model are all relevant to determining what steps would be reasonable when putting in place practices, procedures and systems.

1.32 For instance, where a CDR entity uses outsourced service providers (such as cloud-based service providers for hosting services or data centres and backup providers), the reasonable steps it should take may be different to those it would take if it did not operate in this manner.

## The amount of CDR data handled by the CDR entity

1.33 More rigorous steps may be required as the amount of CDR handled by a CDR entity increases. Generally, as the amount CDR data that is held increases, so too will the steps to ensure that it is reasonable.

### Adverse consequences for a consumer

1.34 Entities should consider the possible adverse consequences for the consumers concerned if the CDR data is not handled in accordance with the CDR Regime. For example, the nature of the CDR data or amount of data held could result in material harm from identity theft or fraud, discrimination, or humiliation or embarrassment. The likelihood of harm occurring will be relevant in considering whether it is reasonable to take a particular step.

### Practicability of implementation

1.35 The practicality of implementing, including the time and cost involved, will influence the reasonableness. A 'reasonable steps' test recognises that privacy protection should be viewed in the context of the practical options available to a CDR entity.

1.36 However, a CDR entity is not excused from implementing particular practices, procedures or systems by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take a particular step will depend on whether the burden is excessive in all the circumstances.

1.37 CDR entities are also not excused from any specific processes, procedures or systems that are required by the CDR Regime.

# Having a CDR policy

## Developing the CDR policy

1.38 CDR policies are a key tool for ensuring open and transparent management of personal information which can build trust and engage consumers.

1.39 Privacy Safeguard 1 requires CDR entities to have a clearly expressed and up-to-date CDR policy about how they manage CDR data. The policy must be distinct from any of the CDR entity's privacy policies,[7] for example, by being contained in a separate document to the entity's privacy policy.

1.40 At a minimum, a CDR policy should be clearly expressed. Specifically, it should be easy to understand (avoiding jargon, legalistic and in-house terms), easy to navigate, and only include information that is relevant to the management of CDR data by the entity.

1.41 A CDR entity must regularly review and update its CDR policy to ensure that it reflects the entity's CDR data handling practices. This review should, at a minimum, be undertaken as part of annual planning processes. An entity could also:

- include a notation on the policy indicating when it was last updated
- invite comment on the policy to gain feedback and evaluate its effectiveness, and
- explain how any comments will be dealt with.

1.42 As the Consumer Data Rules require a CDR policy to be available on the entity's website and on an application for mobile device, it should be available in a style and length that makes it suitable for online and mobile friendly publication.

1.43 It is open to a CDR entity to choose the style and format for its CDR policy, so long as the policy is clearly expressed, up-to-date and otherwise compliant with the requirements of Privacy Safeguard 1 and the Consumer Data Rules. This may include the use of innovative formats to best communicate the privacy messaging to consumers, such as the use of infographics, animation or video or other forms of technology to increase user experience. However, when creating a CDR policy, entities should remember that the key objective is to be transparent with consumers about the handling of CDR data.

[7] Rule 7.2(2).

1.44 Using a layered approach to provide the information may assist a consumer's understanding of the information in the policy. A layered approach means providing a condensed version of the full policy to outline key information, with direct links to the more detailed information in the full policy.[8]

# Information that must be included in a CDR policy

1.45 Privacy Safeguard 1 contains a non-exhaustive list of information that a CDR entity must include in its CDR policy. Additional requirements for each CDR entity are set out in the Consumer Data Rules.

1.46 There are different requirements depending on whether the CDR entity is an accredited data recipient, a data holder, or a designated gateway.

1.47 Where an entity occupies more than one role in the CDR regime (for example is both a data holder and an accredited data recipient), the entity can either have a single CDR policy that outlines how CDR data is handled in both capacities, or a separate CDR policy for each capacity.

## Accredited data recipients

1.48 Privacy Safeguard 1 requires that accredited data recipients must include the following in their CDR policy:

- classes[9] of CDR data held. The *Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019* (the Designation) sets out three classes of information for the banking sector: customer information'[10], product use information[11], and Information on the product'. [12]
- how the CDR data is held
- purposes for which an entity can collect, hold, use or disclose CDR data
- how a consumer may access or correct CDR data
- how a consumer can complain and how the entity will deal with a complaint
- whether overseas disclosure is likely
- circumstances in which the CDR entity may disclose CDR data to a person who is not an accredited person[13]
- events about which the CDR entity will notify the consumers of such CDR data
- when the entity must delete or de-identify CDR data in accordance with a request by a consumer.

[8] For an example of a layered approach, see OAIC, Summary of the OAIC's APP Privacy Policy, OAIC website <www.oaic.gov.au>.

[9] The classes of information are set out in the designation instrument for the relevant sector.

[10] Specified in section 6 of the Designation

[11] Specified in section 7 of the Designation

[12] Specified in section 8 of the Designation

[13] An accredited data recipient is not authorised to disclose to any person who is not an accredited person except directly to the consumer, or where the person is an outsourced service provider

1.49 In addition, the Consumer Data Rules provide other matters that must be included in the CDR policy, including:

- A statement indicating the consequences to the consumer if they withdraw a consent to collect or to use CDR data. This could include information about any early cancellation fees.
- A list of outsourced service providers, the nature of their services, the CDR data and classes of CDR data that may be disclosed.
- Where the accredited data recipient is likely to disclose CDR data overseas to a service provider who is not accredited, a list of countries in which the overseas persons are likely to be based (if it is practicable to specify those countries in the policy).[14]
- Where the accredited data recipient proposes to store CDR data other than in Australia or an external territory, the countries in which the accredited data recipient proposes to store CDR data.
- Where the accredited data recipient seeks or intends that it will seek consent from consumers to de-identify their CDR data in accordance with Consumer Data Rule 4.11(3)(e):
  - why the accredited data recipient asks for consents to de-identify CDR data
  - how the accredited data recipient de-identifies CDR data, including a description of techniques that it uses to de-identify CDR data
  - if the accredited data recipient ordinarily discloses (by sale or otherwise) de-identified CDR data to one or more persons: the fact of this disclosure; the classes of persons such data is ordinarily disclosed to; and the purposes for which the accredited data recipient discloses de-identified CDR data.
- When and how the accredited data recipient destroys 'redundant data', and how a consumer may elect for the accredited data recipient to destroy their CDR data when it becomes redundant data.
- Where the accredited data recipient has a general policy of de-identifying CDR data once it becomes redundant data:
  - if the accredited data recipient uses the de-identified CDR data, examples of how the accredited data recipient ordinarily uses de-identified CDR data
  - how the accredited data recipient de-identifies CDR data, including a description of techniques that it uses to de-identify CDR data
  - if the accredited data recipient ordinarily discloses (by sale or otherwise) de-identified CDR data to one or more persons: the fact of this disclosure; the classes of

[14] An example of when it may be impracticable to specify the countries in which service providers are likely to be located is where CDR data is likely to be disclosed to numerous overseas service providers and the burden of determining where those service providers are likely to be located is excessively time-consuming, costly or inconvenient in all the circumstances. However, an accredited data recipient is not excused from specifying the countries by reason only that it would be inconvenient, time-consuming or impose some cost to do so. It is the responsibility of the accredited data recipient to be able to justify that this is impracticable. If CDR data is disclosed to numerous overseas locations, one practical option may be to list those countries in an appendix to the CDR policy rather than in the body of the policy. Another option in these circumstances may be to include a link in the CDR policy to a regularly updated list of those countries, accessible from the accredited data recipient's website. Where it is not practicable to specify the countries, the accredited data recipient could instead identify general regions (such as European Union countries).

persons such data is ordinarily disclosed to; and the purposes for which the accredited data recipient discloses de-identified CDR data.

- Further information regarding how a consumer can complain and how the accredited data recipient will deal with the complaint, specifically:
  - where, how and when a complaint can be lodged
  - when a consumer should expect an acknowledgement of their complaint
  - what information is required from the complainant
  - the complaint handling process, including time periods associated with the various stages
  - options for redress
  - options for review.

## Data holder

1.50 Privacy Safeguard 1 requires that data holders must include in their CDR policy how a consumer can access and correct the CDR data, and how they may complain.

1.51 In addition, the Consumer Data Rules provide other matters that must be included in the CDR policy, including:

- whether the data holder accepts consumer data requests for voluntary product data or voluntary consumer data, and, if so whether the data holder charges fees for disclosure of such data and what those fees are[15]
- how a consumer can complain and how the entity will deal with a complaint, specifically:
  - where, how and when a complaint can be lodged
  - when a consumer should expect an acknowledgement of their complaint
  - information required from the complainant
  - complaint handling process, including time periods associated with the various stages
  - options for redress
  - options for review.

## Designated gateway

1.52 Privacy Safeguard 1 requires that designated gateways must include the following in their CDR policy:

- an explanation of how the entity will act between persons to facilitate the disclosure of the CDR data, the accuracy of the CDR data, or any other matters required under the Consumer Data Rules

[15] Voluntary product data means CDR data for which there are no consumers that is not required product data: Consumer Data Rules Schedule 3, clause 3.1. Voluntary consumer data means CDR data for which there are consumers that is not required consumer data: Consumer Data Rules Schedule 3, clause 3.2.

- how a consumer may complain about a failure of the CDR entity to comply with the Privacy Safeguards or the Consumer Data Rules, and how the CDR entity will deal with such a complaint.

## Availability of the CDR policy

1.53 The CDR policy must be publicly and freely available in accordance with the Consumer Data Rules.[16] This furthers the objective of Privacy Safeguard 1 of ensuring that CDR data is managed in an open and transparent way.

1.54 The Consumer Data Rules provide that the CDR policy must be readily available on each online platform where the CDR entity ordinarily deals with consumers. For example, where an entity ordinarily deals with consumers through websites and mobile applications, the CDR policy must be readily available on each of the entity's websites and each application for mobile device.

1.55 The CDR policy should be prominently displayed, accessible and easy to download. For example, a prominent link or icon, displayed on relevant pages of the entity's website or mobile application, could provide a direct link to the CDR policy.

1.56 Appropriate accessibility measures should be put in place so that the policy may be accessed by consumers with special needs (such as consumers with a vision impairment, or consumers from a non-English speaking background). While these accessibility measures would not necessarily have to be available online or in a mobile application, there needs to be a clear and accessible method to contact to entity and request this information.

## Consumer requests for a CDR policy

1.57 If a copy of the CDR entity's policy is requested by a consumer for the CDR data, the CDR entity must give the consumer a copy in accordance with Consumer Data Rule 7.2.

1.58 The Consumer Data Rules provide that, if requested by consumer, the CDR entity must give the consumer a copy of the policy electronically or hard copy as requested by the consumer.

[16] 56ED (7)